

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF
INFORMATION THAT IS STORED AT
PREMISES CONTROLLED BY GOOGLE
LLC, 1600 AMPHITHEATRE PARKWAY,
MOUNTAIN VIEW, CALIFORNIA 94043

FILED UNDER SEAL

Case No. 21-mj-225-01-DL

AFFIDAVIT

I, John Forte, having been duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search information that is stored at premises controlled by Google, an electronic communication service and remote computing service provider headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government the information further described in Attachment B.I. The government will then review that information and seize the information that is further described in Attachment B.II.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), United States Department of Justice, and have been so employed since 2002. I am currently assigned to the ATF Boston Field Division, Manchester, New Hampshire Field Office, and charged with investigating criminal offenses involving the federal firearms, explosives, arson, alcohol, and tobacco diversion laws.

3. I have received extensive training in the federal firearms laws and am familiar with ATF's regulations regarding the purchase and sales of firearms. I have successfully

completed the Criminal Investigations Training Program and the ATF New Professional Training (NPT) at the Federal Law Enforcement Training Center in Glynco, GA. During the NPT program, I learned how to investigate criminal offenses involving the federal firearms, explosives, arson, alcohol, and tobacco diversion laws. I have received advanced training with regard to conducting complex firearms trafficking investigations. I have participated in dozens of investigations relating to the illegal acquisition and sales of firearms, the illegal manufacture and possession of National Firearms Act weapons and previously have sworn out numerous affidavits in support of search warrants and arrest warrants in firearms cases. I have been certified as an Interstate Nexus Expert, that is, an expert in establishing whether particular firearms or ammunition have traveled in interstate commerce thereby satisfying the interstate commerce element of many federal firearms crimes.

4. The information contained within this affidavit is based upon my training, experience, and investigation, as well as information that has been conveyed to me by other law enforcement officers and witnesses. The following is either known to me personally or has been related to me by persons having direct knowledge of the events described below, including other law enforcement officers involved in this investigation. Since this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to me concerning this investigation.

5. Based on the facts set forth in this affidavit, there is probable cause to search the information described in Attachment A for evidence of violations of Title 18, United States Code, United States Code, Section 922(u), theft of a firearm(s) from a Federal firearms licensee (hereinafter, "FFL"). Based on the facts set forth in this affidavit, I submit there is probable cause that violations of 18 U.S.C. §922(u) occurred.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

7. Based on my training and experience, I know that cellular devices, such as mobile telephones, are wireless devices that enable their users to send or receive wire and/or electronic communications using the networks provided by cellular service providers. Using cellular networks, users of many cellular devices can send and receive communications over the Internet.

8. I also know that many devices, including but not limited to cellular devices, have the ability to connect to wireless Internet (“wi-fi”) access points if the user enables wi-fi connectivity. These devices can, in such cases, enable their users to send or receive wire and/or electronic communications via the wi-fi network. A tablet such as an iPad is an example of a device that may not have cellular service but that could connect to the Internet via wi-fi. Wi-fi access points, such as those created through the use of a router and offered in places like homes, hotels, airports, and coffee shops, are identified by a service set identifier (“SSID”) that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device’s wi-fi settings.

9. Based on my training and experience, I also know that many devices, including many cellular and mobile devices, feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a device such as a cellular phone

or tablet and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by devices within the Bluetooth device's transmission range, to which it might connect.

10. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the device can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the apps' operation.

11. Based on my training and experience, I know Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every device using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

12. In addition, based on my training and experience, I know that Google offers numerous apps and online-based services, including messaging and calling (e.g., Gmail, Hangouts, Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage, and sharing (e.g., Drive, Keep, Photos, and YouTube). Many of these services are accessible only to users who have signed in to their Google accounts. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address (e.g., example@gmail.com). Other services, such as Maps and YouTube, can be used with limited functionality without the user being signed in to a Google account.

13. Based on my training and experience, I also know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user has

the ability to sign-in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be uploaded to Google and then synced across the various devices on which the subscriber may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices and Windows computers, among others.

14. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices.

15. According to my training and experience, as well as open-source materials published by Google, I know that Google offers accountholders a service called "Location History," which authorizes Google, when certain prerequisites are satisfied, to collect and retain a record of the locations where Google calculated a device to be based on information transmitted to Google by the device. That Location History is stored on Google servers, and it is associated with the Google account that is associated with the device. Each accountholder may view their Location History and may delete all or part of it at any time.

16. Based on my training and experience, I know that the location information collected by Google and stored within an account's Location History is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device. Google uses this information to calculate the device's estimated latitude and longitude, which varies in its accuracy depending on the source of the data. Google records the

margin of error for its calculation as to the location of a device as a meter radius, referred to by Google as a “maps display radius,” for each latitude and longitude point.

17. Based on open-source materials published by Google and my training and experience, I know that Location History is not turned on by default. A Google accountholder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account in order for that usage to be recorded in Location History. A Google accountholder can also prevent additional Location History records from being created at any time by turning off the Location History setting for their Google account or by disabling location reporting for a particular device or Google application. When Location History is enabled, however, Google collects and retains location data for each device with Location Services enabled, associates it with the relevant Google account, and then uses this information for various purposes, including to tailor search results based on the user’s location, to determine the user’s location when Google Maps is used, and to provide location-based advertising. As noted above, the Google accountholder also has the ability to view and, if desired, delete some or all Location History entries at any time by logging into their Google account or by enabling auto-deletion of their Location History records older than a set number of months.

18. Location data, such as the location data in the possession of Google in the form of its users’ Location Histories, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected and retained via the use of Google products as described above, devices that were likely in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this

information can indicate that a Google accountholder was near a given location at a time relevant to the criminal investigation by showing that his/her device reported being there.

19. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provide clues to their identity, location, or illicit activities.

20. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

21. Google assigns an "anonymized" number, known as the Device ID or Obfuscated

ID, to a device, and the location data associated with a Device ID is never deleted. These data are available to law enforcement through the issuance of a probable cause search warrant. To obtain this information, Google requires a timeframe and general location, established either through a latitudinal/longitudinal point with a given radius or a polygon-shaped area with the latitude and longitude for each point of the polygon.

MILFORD FIREARMS BURGLARY

22. On August 31, 2021, at approximately 3:56 AM, a dark-colored sedan and a light-colored sport utility vehicle (SUV) pulled into the parking lot of Milford Firearms located at 286 Elm Street in Milford, New Hampshire (also NH Route 101A). Milford Firearms is a federal firearms licensee (FFL) which is licensed to sell/transfer firearms to the general public. Three individuals exited the two vehicles and proceeded to break into Milford Firearms via the glass front door. Upon making entry into the interior of Milford Firearms, the three suspects used a tool to smash the glass display cabinets which housed numerous handguns. The suspects proceeded to steal seventeen firearms from Milford Firearms based upon an inventory conducted by employees of Milford Firearms and ATF Industry Operations Investigators.

23. The three suspects then exited Milford Firearms and got back into the two vehicles previously described. The two suspect vehicles then exited the parking lot and proceeded East on Elm Street. The entirety of the burglary lasted less than a minute.

24. On that same day, investigators began a neighborhood canvass of the area around Milford Firearms and the direction of travel for the suspect vehicles. Investigators reviewed security camera footage for the Milford Town Hall which is located at 1 Union Square in Milford, NH and noted that at approximately 3:53 AM EST, a vehicle matching the description of the suspect vehicles travelled West in the direction of Milford Firearms. At approximately

3:58 AM EST, a vehicle matching the description of the suspect vehicles travelled East on NH Route 101A from Elm Street away from the direction of Milford Firearms. It should be noted that Elm Street turns into Nashua Street at the intersection of Union Square in Milford, NH, but still remains NH Route 101A.

25. Investigators also located security camera footage from the Mobil gas station located at 75 NH Route 101A in Amherst, NH which showed both of the suspect vehicles travelling East on NH Route 101A at approximately 4:03AM EST on August 31, 2021.

26. Investigators also located security camera footage from the St. Mary's Bank located at 4 Northwest Boulevard (NH Route 101A) in Nashua, NH that showed vehicles that matched the description of both suspect vehicles pass the location at approximately 4:08 AM EST on August 31, 2021, travelling East.

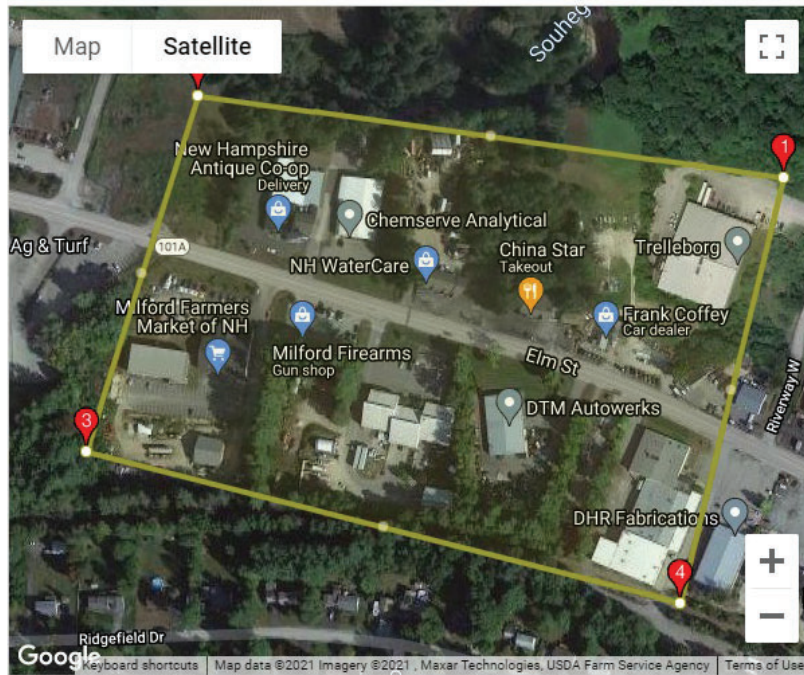
27. Investigators also located security camera footage from the Mobil gas station located at 242 Amherst Street in Nashua, NH that showed vehicles that matched the description of both suspect vehicles pass the location at approximately 4:11 AM EST headed East on NH Route 101A.

28. At the time the burglary occurred, Milford Firearms was closed and no store employees or their smartphones were present.

29. An initial review of the router in Milford Firearms indicated that it had captured a log containing a number of MAC addresses in it's memory. Investigators noted that there are no timestamps associated with the log of the MAC addresses to assist in narrowing down the MAC addresses captured at the time of the burglary.

TECHNICAL INFORMATION

30. On August 31, 2021, I identified the following coordinates for Target Location #1, being 286 Elm Street in the town of Milford, NH. Target Location #1 is the geographical area identified as a polygon defined by the following latitude/longitude coordinates and connected by straight lines:



Point 1: 42.841040, -71.671051

Point 2: 42.841520, -71.675729

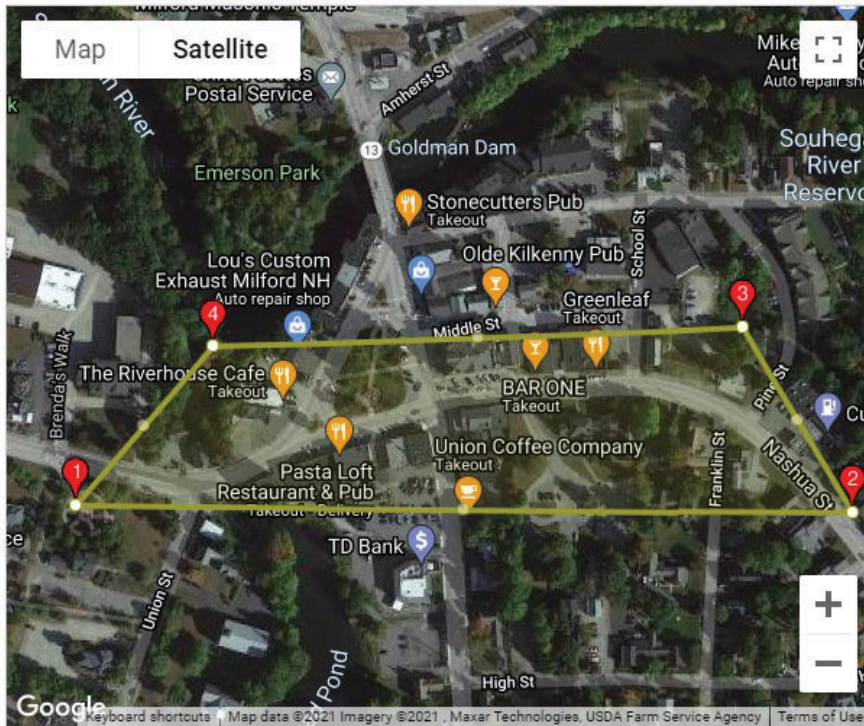
Point 3: 42.839435, -71.676619

Point 4: 42.838546, -71.671877

31. The Google geofence information for Target Location #1 is being requested during the following time period in which investigators believe the suspects committed the burglary at the FFL, on August 31, 2021 at approximately 3:56 AM EST.

32. On August 31, 2021, I identified the following coordinates for Target Location #2, being 1 Union Square in the town of Milford, NH. Target Location #2 is the geographical

area identified as a polygon defined by the following latitude/longitude coordinates and connected by straight lines:



Point 1: 42.834897, -71.651807

Point 2: 42.834858, -71.646045

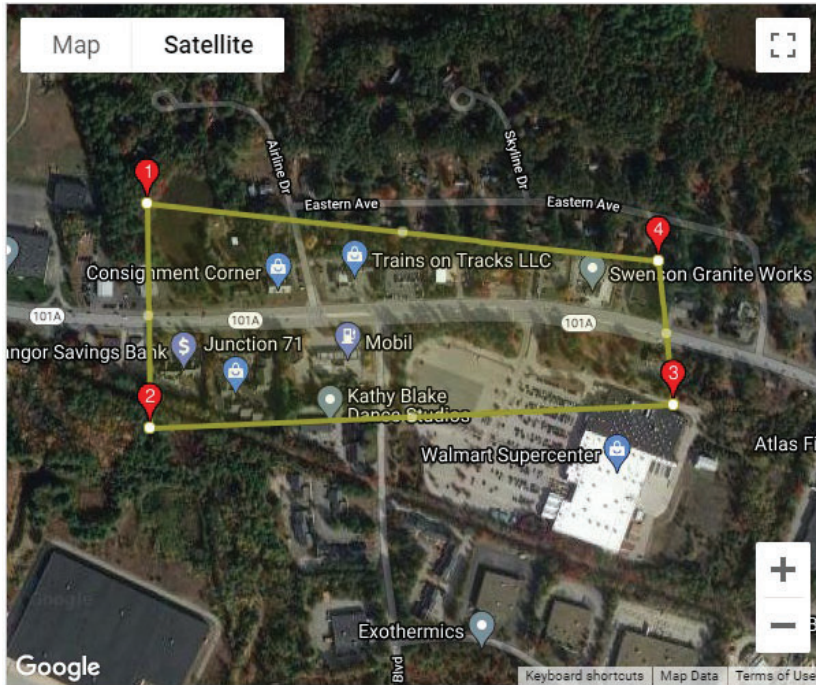
Point 3: 42.835865, -71.646861

Point 4: 42.835762, -71.650787

33. The Google geofence information for Target Location #2 is being requested during the following time period in which investigators believe the suspects travelled to and from the burglary location along NH Route 101A, on August 31, 2021, at approximately 3:53 AM EST and again at 3:58 AM EST.

34. On August 31, 2021, I identified the following coordinates for Target Location #3, being 75 NH Route 101 in the town of Amherst, NH. Target Location #3 is the geographical

area identified as a polygon defined by the following latitude/longitude coordinates and connected by straight lines:



Point 1: 42.812683, -71.586633

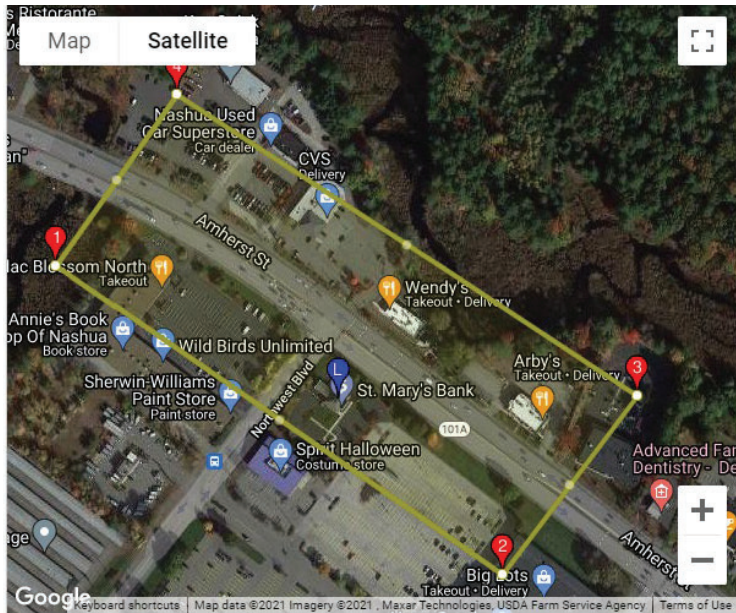
Point 2: 42.810101, -71.586590

Point 3: 42.810369, -71.578371

Point 4: 42.812022, -71.578607

35. The Google geofence information for Target Location #3 is being requested during the following time period in which investigators believe the suspects travelled from the burglary location along NH Route 101A, on August 31, 2021, at approximately 4:03 AM EST.

36. On August 31, 2021, I identified the following coordinates for Target Location #4, being 4 Northwest Boulevard in the city of Nashua, NH. Target Location #4 is the geographical area identified as a polygon defined by the following latitude/longitude coordinates and connected by straight lines:



Point 1: 42.803543, -71.543479

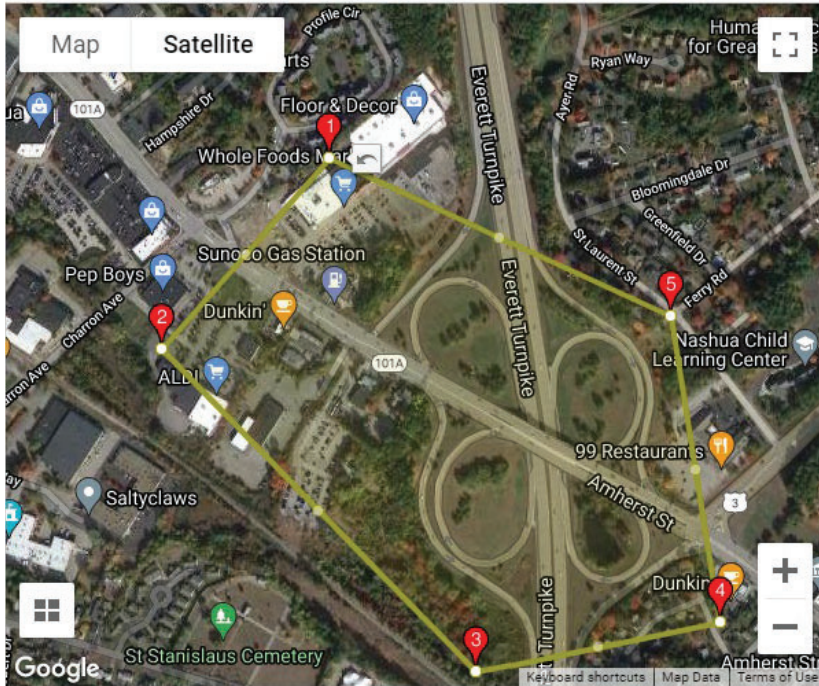
Point 2: 42.801559, -71.539563

Point 3: 42.802709, -71.538383

Point 4: 42.804645, -71.542417

37. The Google geofence information for Target Location #4 is being requested during the following time period in which investigators believe the suspects travelled from the burglary location along NH Route 101A, on August 31, 2021, at approximately 4:08 AM EST.

38. On August 31, 2021, I identified the following coordinates for Target Location #5, being 242 Amherst Street in the city of Nashua, NH. Target Location #5 is the geographical area identified as a polygon defined by the following latitude/longitude coordinates and connected by straight lines:



Point 1: 42.780072, -71.496365

Point 2: 42.777883, -71.498983

Point 3: 42.774181, -71.494070

Point 4: 42.774748, -71.490250

Point 5: 42.778261, -71.491023

39. The Google geofence information for Target Location #5 is being requested during the following time period in which investigators believe the suspects travelled to and from the burglary location along NH Route 101A, on August 31, 2021, at approximately 4:11 AM EST.

40. This application requests a warrant as the first step of a two-step process. The data being provided in the execution of the requested warrant is anonymized. Google would only provide the “Device ID” or “Obfuscated ID” information and there is no method for this affiant or other law enforcement investigators to identify the related user(s) of the device(s) with this information alone. Once the data have been received from Google, investigators will

process the data to identify any “Device ID(s)” that appear to be related to the specific crime being investigated, based on the presence or absence of the devices at specific times. If relevant “Device ID(s)” are identified, an application for a second search warrant related to the specific “Device ID(s)” that were discovered will be submitted to seek additional identification information in reference to those “Device ID(s).” This additional information may include: owner/user identifiers, extended location history, and/or additional device identifiers.

CONCLUSION

Based on the foregoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, and because this warrant seeks only permission to examine electronic records and does not involve the intrusion onto physical premises, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

/s/ John Forte

John Forte
Special Agent, ATF

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: 9/2/2021
Time: 9:25 a.m.



Hon. Daniel J. Lynch
United States Magistrate Judge

ATTACHMENT A

Property To Be Searched

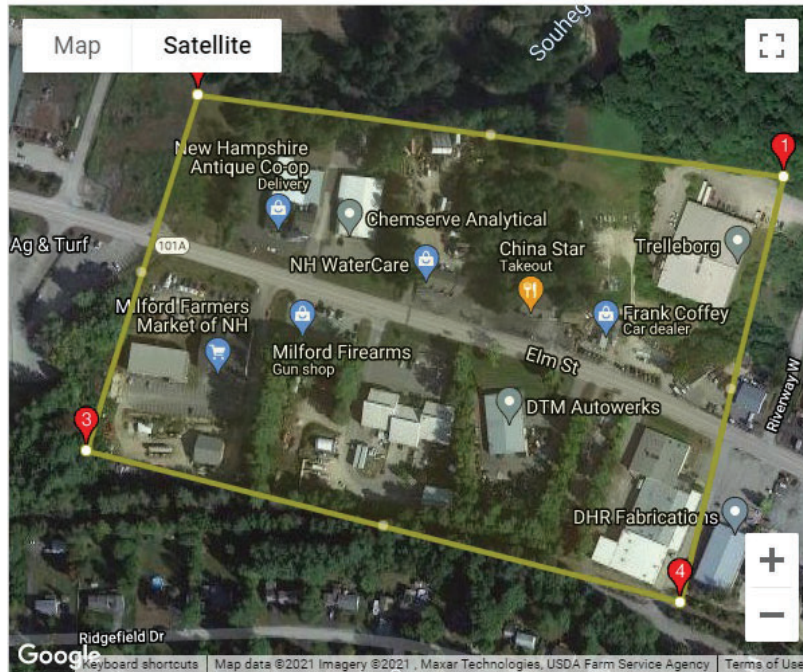
This warrant is directed to Google LLC and applies to:

- (1) Location History data, sourced from information including GPS data and information about visible wi-fi points and Bluetooth beacons transmitted from devices to Google, reflecting devices that Google calculated were or could have been (as indicated by margin of error, *i.e.*, “maps display radius”) located within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below (“Initial Search Parameters”); and
- (2) identifying information for Google Accounts associated with the responsive Location History data.

Initial Search Parameters

Search Parameter 1 – 286 Elm Street, Milford, New Hampshire

- Date: August 31, 2021
- Time Periods (including time zone):
 - 3:41 AM EST through 4:11 AM EST
- Target Location: Geographical area identified as:
 - A polygon defined by the following latitude/longitude coordinates connected by straight lines:



Point 1: 42.841040, -71.671051

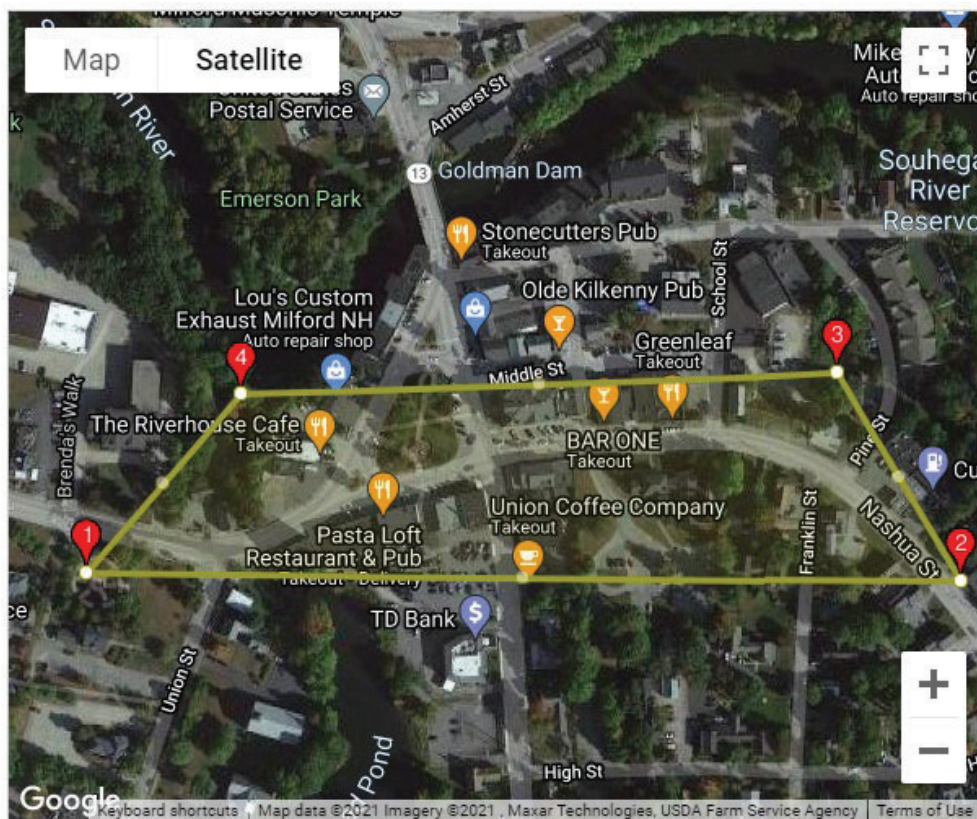
Point 2: 42.841520, -71.675729

Point 3: 42.839435, -71.676619

Point 4: 42.838546, -71.671877

Search Parameter 2 – 1 Union Square, Milford, New Hampshire

- Date: August 31, 2021
- Time Periods (including time zone):
 - 3:38 AM EST through 4:13 AM EST
- Target Location: Geographical area identified as:
 - A polygon defined by the following latitude/longitude coordinates connected by straight lines:



Point 1: 42.834897, -71.651807

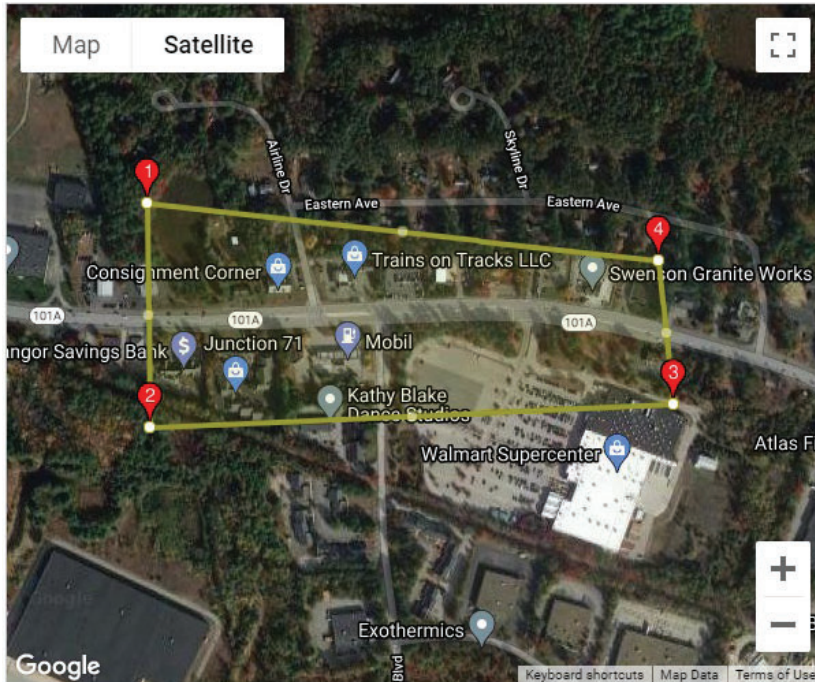
Point 2: 42.834858, -71.646045

Point 3: 42.835865, -71.646861

Point 4: 42.835762, -71.650787

Search Parameter 3 – 75 NH Route 101A, Amherst, New Hampshire

- Date: August 31, 2021
- Time Periods (including time zone):
 - 3:34 AM EST through 4:18 AM EST
- Target Location: Geographical area identified as:
 - A polygon defined by the following latitude/longitude coordinates connected by straight lines:



Point 1: 42.812683, -71.586633

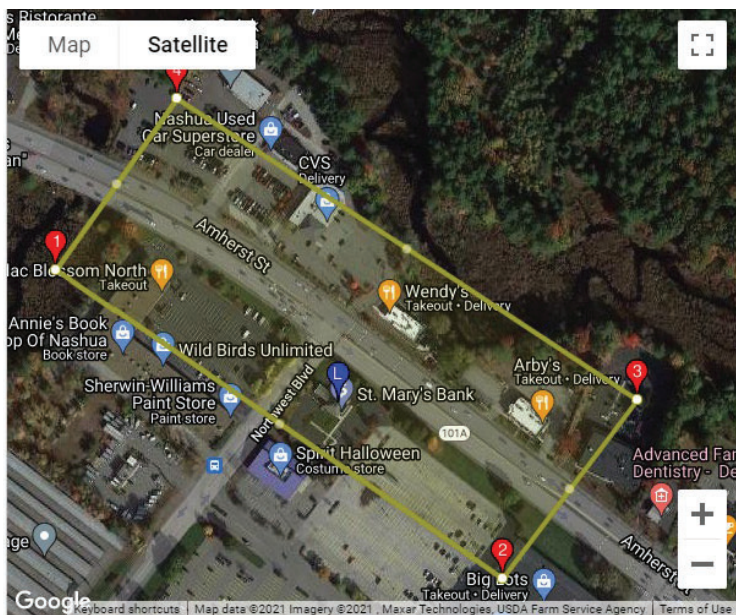
Point 2: 42.810101, -71.586590

Point 3: 42.810369, -71.578371

Point 4: 42.812022, -71.578607

Search Parameter 4 – 4 Northwest Boulevard, Nashua, New Hampshire

- Date: August 31, 2021
- Time Periods (including time zone):
 - 3:29 AM EST through 4:23 AM EST
- Target Location: Geographical area identified as:
 - A polygon defined by the following latitude/longitude coordinates connected by straight lines:



Point 1: 42.803543, -71.543479

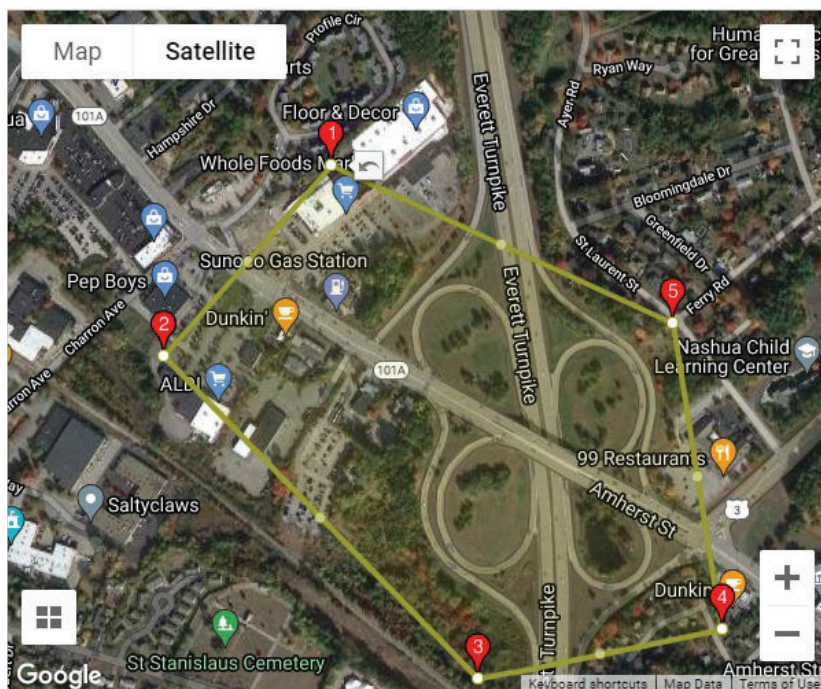
Point 2: 42.801559, -71.539563

Point 3: 42.802709, -71.538383

Point 4: 42.804645, -71.542417

Search Parameter 5 – 242 Amherst Street, Nashua, New Hampshire

- Date: August 31, 2021
- Time Periods (including time zone):
 - 3:26 AM EST through 4:26 AM EST
- Target Location: Geographical area identified as:
 - A polygon defined by the following latitude/longitude coordinates connected by straight lines:



Point 1: 42.780072, -71.496365

Point 2: 42.777883, -71.498983

Point 3: 42.774181, -71.494070

Point 4: 42.774748, -71.490250

Point 5: 42.778261, -71.491023

ATTACHMENT B

Particular Items to Be Seized

I. Information to be disclosed by Google

The information described in Attachment A, via the following process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A. For each location point recorded within the Initial Search Parameters, and for each location point recorded outside the Initial Search Parameters where the margin of error (*i.e.*, “maps display radius”) would permit the device to be located within the Initial Search Parameters, Google shall produce to the government information specifying the corresponding unique device ID, timestamp, location coordinates, display radius, and data source, if available (the “Device List”).
2. The government shall review the Device List and identify to Google the devices about which it seeks to obtain Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.
3. Google shall disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Accounts associated with each device ID appearing on the Device List about which the government inquires.

II. Information to Be Seized

All information described above in Section I that constitutes evidence of violations of Title 18, United States Code, Sections 371 and 924(m), conspiracy and theft of firearm(s) from a Federal firearms licensee, have been committed on August 31, 2021, involving unknown person(s).